E.S.E.
RAFAEL TOVAR POVEDA
NIT. 900211477-1

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2026

TABLA DE CONTENIDO

1. OBJETIVOS

OBJETIVO GENERAL

Establecer, implementar, mantener y mejorar de forma continua el Plan de Seguridad y Privacidad de la Información de la E.S.E. RAFAEL TOVAR POVEDA, alineado con los principios de la NORMA ISO/IEC 27001:2022 (International Organization for Standardization & International Electrotechnical Commission [ISO/IEC], 2022a), y con la normatividad del sector salud, con el fin de gestionar adecuadamente los riesgos que afectan la confidencialidad, integridad y disponibilidad de la información y apoyar la prestación segura y oportuna de los servicios de la E.S.E.

OBJETIVOS ESPECIFICOS

- Definir el contexto, alcance, estructura de gobierno, roles y responsabilidades para la gestión de la seguridad y privacidad de la información, incluyendo la creación y funcionamiento del Comité de Seguridad de la Información (CSI).
- Establecer y mantener una metodología para la identificación, inventario, clasificación y valoración de los activos de información, así como para la gestión de riesgos de seguridad de la información, generando y actualizando la matriz de riesgos, el Plan de Tratamiento de Riesgos y la Declaración de Aplicabilidad.
- Diseñar, documentar, revisar y aprobar políticas, normas y procedimientos que regulen el uso y la protección de los activos de información, equipos, redes, aplicaciones, medios físicos y canales de comunicación, en coherencia con el SGSI y el Sistema de Gestión de la Calidad institucional.
- Implementar controles organizacionales, de personal, físicos y tecnológicos que reduzcan los riesgos de seguridad de la información a niveles aceptables, de acuerdo con los resultados del análisis de riesgos y con la disponibilidad de recursos definidos por la Alta Dirección.
- Promover la concientización, formación y cambio cultural en seguridad de la información y protección de datos personales para todos los directivos,

funcionarios, contratistas y terceros que tengan relación con la E.S.E., fortaleciendo sus responsabilidades frente al uso adecuado de la información y de los recursos tecnológicos.

- Garantizar el cumplimiento de los requisitos legales, regulatorios, contractuales, sectoriales y normativos aplicables en materia de seguridad de la información, protección de datos personales y gestión documental, procurando la trazabilidad de las decisiones y acciones adoptadas.
- Establecer lineamientos para la gestión de incidentes de seguridad de la información, vulnerabilidades, copias de respaldo, continuidad y recuperación de servicios críticos, asegurando la oportuna atención de eventos que afecten la confidencialidad, integridad o disponibilidad de la información.
- Implementar mecanismos de monitoreo, medición, auditoría interna y revisión por la dirección que permitan evaluar el desempeño del Plan de Seguridad y Privacidad de la Información y del SGSI, e impulsar acciones de corrección y mejora continua.

2. ALCANCE

Las directrices de este Plan cubren todos los aspectos administrativos, técnicos y de control que deben ser cumplidos por los directivos, colaboradores, contratistas, terceros y otros actores que laboren o tengan relación con la E.S.E. RAFAEL TOVAR POVEDA, para conseguir un adecuado nivel de protección de la información institucional.

DESDE: Todos los directivos, funcionarios, contratistas, terceros y otros colaboradores de la E.S.E. RAFAEL TOVAR POVEDA, incluyendo personal externo con equipos o dispositivos conectados a la red institucional o que accedan a la información de la E.S.E. de manera local o remota.

HASTA: Todos los equipos, sistemas, aplicaciones, bases de datos, servicios y canales de comunicación que, de alguna manera, utilicen local o remotamente la red institucional o recursos tecnológicos de la E.S.E., así como los servicios de intercambio de archivos y programas y los repositorios físicos de información.

Aplica a todas las sedes de la E.S.E. y a todos los procesos misionales, estratégicos y de apoyo que gestionen información institucional o de usuarios de servicios de salud.

3. NORMATIVIDAD

Este Plan se fundamenta, entre otros, en los siguientes referentes normativos y técnicos (actualizables según cambios posteriores):

- Constitución Política de Colombia (artículos 15, 20 y concordantes – hábeas data y derecho a la intimidad).
- Ley 1581 de 2012 – Protección de datos personales y sus decretos reglamentarios.
- Ley 1266 de 2008 – Régimen de habeas data financiero (cuando aplique).
- Ley 594 de 2000 – Ley General de Archivos.
- Ley 1273 de 2009 – Protección de la información y de los datos.
- Normatividad del sector salud aplicable a la historia clínica y protección de la información del paciente (Resoluciones y circulares vigentes).
- ISO/IEC 27001:2022 – Sistemas de Gestión de Seguridad de la Información (SGSI).
- ISO/IEC 27002:2022 – Código de buenas prácticas para controles de seguridad de la información.
- ISO/IEC 13335-1:2004 – Directrices de gestión de seguridad de TI.
- Política de Seguridad de la Información de la E.S.E. RAFAEL TOVAR POVEDA aprobada por resolución interna.

- Demás normas internas (manual de calidad, reglamento interno de trabajo, manual de funciones, lineamientos de protección de datos personales, etc.).
- Decreto 612 de 2018 y Política de Seguridad Digital (CONPES 3995 de 2020).

4. DEFINICIONES

Activo de información: cualquier componente (humano, tecnológico, de software, documental o de infraestructura) que soporta uno o más procesos de negocio de la E.S.E. y que, por tanto, debe ser protegido.

Acuerdo de confidencialidad: documento mediante el cual colaboradores y contratistas se comprometen a no divulgar ni utilizar indebidamente la información confidencial a la que tienen acceso.

Análisis de riesgos de seguridad de la información: proceso sistemático de identificación de amenazas, vulnerabilidades, impactos y probabilidades para determinar el riesgo sobre la confidencialidad, integridad y disponibilidad de la información.

Autenticación: procedimiento de verificación de la identidad de un usuario o recurso tecnológico para permitir el acceso a un sistema o información.

Capacidad: proceso para determinar la capacidad de los recursos tecnológicos que necesita la entidad para satisfacer las necesidades de procesamiento con rendimiento adecuado.

Centro de cómputo / centros de cableado: áreas físicas destinadas a alojar equipos de procesamiento y comunicaciones, que deben cumplir requisitos de seguridad física, eléctrica y ambiental.

Cifrado: transformación de datos mediante técnicas criptográficas para asegurar su confidencialidad e integridad.

Confidencialidad: propiedad por la cual la información no está disponible o revelada a individuos, entidades o procesos no autorizados.

Disponibilidad: capacidad de que la información y los activos asociados estén accesibles y utilizables por usuarios autorizados cuando lo requieran.

Integridad: propiedad que protege la exactitud, completitud y vigencia de los activos de información.

SGSI: Sistema de Gestión de Seguridad de la Información, estructurado según ISO/IEC 27001.

Usuario: directivo, colaborador, contratista o tercero autorizado para usar equipos, sistemas o aplicativos informáticos de la E.S.E.

Vulnerabilidad: debilidad que puede ser explotada por una amenaza para afectar la confidencialidad, integridad o disponibilidad de la información.

Software malicioso (malware): programas o código hostil (virus, gusanos, troyanos, spyware, ransomware, etc.) que pretende infiltrarse o dañar recursos tecnológicos.

Token de seguridad / firma digital: dispositivo o mecanismo criptográfico que soporta la autenticación fuerte y la firma de transacciones electrónicas.

5. RESPONSABLES

5.1 Alta Dirección

- Aprobar la Política de Seguridad de la Información y el presente Plan.
- Definir y asignar recursos humanos, técnicos y financieros para la gestión de seguridad y privacidad.
- Promover activamente la cultura de seguridad de la información en la E.S.E.
- Establecer procesos disciplinarios frente al incumplimiento de las políticas de seguridad.

5.2 Oficina de Control Interno / Control Interno Disciplinario

- Diseñar y ejecutar el programa de concientización en seguridad de la información.
- Planear y realizar auditorías al SGSI y a los controles de seguridad.
- Emitir recomendaciones sobre soluciones de seguridad y gestión de vulnerabilidades.
- Aplicar el proceso disciplinario cuando se identifiquen violaciones a las políticas.

5.3 Oficina de Sistemas

- Administrar la plataforma tecnológica, redes, sistemas de información y servicios asociados.
- Establecer y aplicar configuraciones seguras, controles de acceso y mecanismos de monitoreo.
- Gestionar cuentas de usuario, perfiles, privilegios y contraseñas.
- Definir y aplicar condiciones de uso para dispositivos móviles, medios de almacenamiento, conexiones remotas, correo electrónico e Internet.

5.4 Otras dependencias

- Talento Humano y Contratación: gestión de acuerdos de confidencialidad, soportes contractuales y procesos de vinculación/desvinculación.
- Gestión Documental: gestión de archivos físicos, tablas de retención, destrucción segura y custodia de medios.
- Recursos Físicos / Activos Fijos: controles de seguridad física, inventario y movimientos de equipos.
- Propietarios de activos de información (subgerencias, coordinaciones, direcciones, jefaturas): definición de perfiles y autorizaciones, clasificación de la información y supervisión de su uso.

5.5 Todos los usuarios

- Cumplir las políticas, normas y procedimientos de seguridad de la información.
- Hacer uso adecuado y responsable de los recursos tecnológicos.
- Reportar de forma oportuna incidentes o sospechas de violaciones de seguridad.

6. DESARROLLO DEL DOCUMENTO

Las actividades descritas en este numeral operacionalizan las políticas y normas de seguridad de la información definidas en el PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (versión 01, 2020), manteniendo su vigencia y articulándolas con los requisitos de la norma ISO/IEC 27001:2022

La secuencia se basa en el ciclo PHVA (Planear – Hacer – Verificar – Actuar) y se alinea con los requisitos normativos ya mencionados para el establecimiento, operación y mejora de un Sistema de Gestión de Seguridad de la Información (SGSI) y con los controles del Anexo A (controles organizacionales, de personas, físicos y tecnológicos).

La implementación de las actividades descritas en este numeral requiere que la E.S.E. RAFAEL TOVAR POVEDA disponga de recursos humanos, tecnológicos, físicos y financieros suficientes. La Alta Dirección será responsable de priorizar y aprobar los recursos necesarios para que los controles definidos en este Plan sean efectivamente implementados y mantenidos.

6.1 Conformación y funcionamiento del Comité de Seguridad de la Información (CSI)

La E.S.E. RAFAEL TOVAR POVEDA conformará un Comité de Seguridad de la Información (CSI) como instancia del Plan de Seguridad y Privacidad de la Información y del Sistema de Gestión de Seguridad de la Información.

El CSI estará integrado, como mínimo, por:

- Gerente.
- Subgerente Administrativa.
- Jefe de la Oficina de Sistemas.
- Jefe de la Oficina de Control Interno.

- Representante del área de Talento Humano.
- Representante de Gestión Documental y Archivo.
- Otros invitados permanentes u ocasionales que la Gerencia considere necesarios.

Funciones principales del CSI:

- Aprobar el Plan de Seguridad y Privacidad de la Información y sus actualizaciones.
- Revisar y recomendar la aprobación de políticas, normas y procedimientos específicos de seguridad de la información.
- Conocer los resultados de la evaluación de riesgos de seguridad de la información y aprobar los planes de tratamiento de riesgos.
- Revisar los informes de incidentes de seguridad de la información y las acciones correctivas y de mejora.
- Hacer seguimiento al cumplimiento de los objetivos de seguridad de la información y a los indicadores definidos.
- Recomendar a la Gerencia las decisiones estratégicas relacionadas con seguridad de la información.
- Informar a la Gerencia los riesgos derivados de la falta de recursos para implementar o mantener controles de seguridad y dejar registro de dichas situaciones en las actas del Comité.

El CSI sesionará con una periodicidad mínima semestral, o de manera extraordinaria cuando se presenten incidentes relevantes o cambios significativos en los riesgos de seguridad de la información.

Mientras se conforma formalmente el CSI, la Gerencia y la Subgerencia Administrativa, con apoyo de la Oficina de Sistemas y la Oficina de Control Interno, asumirán de manera transitoria las funciones descritas en este numeral, dejando registro en actas de reunión de comité de gerencia u órganos de dirección existentes.

6.2 Planeación y actualización del contexto y alcance del Plan

Actividad: Definir y revisar el alcance, objetivos y contexto del Plan de Seguridad y Privacidad de la Información.

Cómo se realiza:

1. Se identifican las partes interesadas (internas y externas) y sus necesidades en materia de seguridad de la información.
2. Se revisan los requisitos legales, reglamentarios, contractuales y normativos aplicables (incluyendo ISO/IEC 27001:2022).
3. Se define o actualiza el alcance del Plan (procesos, sedes, sistemas, información) y los objetivos de seguridad de la información.
4. Se revisan anualmente (o cuando haya cambios significativos) los objetivos, alcance y contexto.

Responsables:

- **Gerencia:** aprueba el alcance y los objetivos del Plan/SGSI, asegura la alineación con la estrategia institucional y decide sobre cambios relevantes de alcance.
- **Oficina de Control Interno:** lidera la identificación de partes interesadas y requisitos, consolida la matriz de contexto y emite recomendaciones sobre riesgos y cumplimiento normativo.
- **Oficina de Sistemas de Información:** aporta información sobre activos tecnológicos, servicios, sistemas y cambios en la infraestructura que impacten el alcance y el contexto del Plan.

Registros resultantes:

- Documento de alcance del Plan / SGSI.
- Matriz de partes interesadas y requisitos.
- Actas donde se aprueban alcance y objetivos.

- Actualizaciones del Plan de Seguridad y Privacidad de la Información.

6.3 Identificación, inventario y clasificación de activos de información

Actividad: Identificar y mantener el inventario de activos de información y su clasificación.

Cómo se realiza:

1. Cada proceso identifica sus activos de información (información, aplicaciones, infraestructura, personas, servicios, etc.).
2. La Oficina de Sistemas de Información y el Área de Activos Fijos consolidan el inventario tecnológico (servidores, estaciones de trabajo, redes, dispositivos móviles, medios de almacenamiento, tokens, etc.).
3. Con base en la guía de clasificación, se asigna a cada activo un nivel de clasificación (por ejemplo: pública, uso interno, restringida, reservada) y se indican propietarios y custodios.
4. Se actualiza el inventario cuando se crean, modifican, trasladan o eliminan activos.

Responsables:

- **Oficina de Sistemas de Información:** consolida el inventario de activos tecnológicos (hardware, software, redes, medios de almacenamiento, dispositivos móviles), mantiene sus atributos técnicos actualizados y apoya la clasificación de activos digitales.
- **Área de Activos Fijos:** administra el inventario contable y físico de equipos y otros bienes, garantiza la coherencia entre el inventario de activos de información y el inventario institucional de activos fijos.
- **Área de Gestión Documental:** administra la clasificación y organización de los documentos físicos y digitales, integra los niveles de clasificación de información al sistema de gestión documental y a las tablas de retención.

Registros resultantes:

- Inventario de activos de información.
- Matriz de propietarios y custodios.
- Guía de clasificación de la información actualizada.

6.4 Evaluación y tratamiento de riesgos de seguridad de la información

Actividad: Realizar la evaluación y tratamiento de riesgos de seguridad de la información de forma periódica y consistente, de acuerdo con ISO/IEC 27001:2022, cláusula 6.1 (ISO/IEC, 2022a).

Cómo se realiza:

1. La Oficina de Control Interno, junto con los propietarios de activos y la Oficina de Sistemas, definen y/o actualizan la metodología de análisis de riesgos (criterios de impacto, probabilidad, niveles de riesgo, etc.).
2. Se identifican amenazas y vulnerabilidades sobre los activos de información, considerando confidencialidad, integridad y disponibilidad.
3. Se valoran los riesgos (probabilidad x impacto) y se priorizan según los criterios definidos.
4. Se definen opciones de tratamiento del riesgo (mitigar, evitar, transferir o aceptar) y los controles correspondientes, alineados con el Anexo A de ISO/IEC 27001:2022.
5. Se elabora y aprueba un Plan de Tratamiento de Riesgos y una Declaración de Aplicabilidad.
6. Se revisan los riesgos periódicamente, y cuando se presenten cambios relevantes (nuevos sistemas, incidentes graves, cambios de procesos, etc.).

La implementación efectiva de la metodología de riesgos y de los planes de tratamiento definidos requerirá que la Alta Dirección priorice y asigne los recursos necesarios (incluyendo, cuando se requiera, apoyo especializado externo), de acuerdo con los niveles de riesgo identificados y las capacidades de la E.S.E.

Responsables:

- **Oficina de Control Interno:** define y actualiza la metodología de análisis de riesgos (criterios, escalas, matriz), coordina las sesiones de identificación y valoración de riesgos y consolida la matriz de riesgos y el Plan de Tratamiento.
- **Oficina de Sistemas de Información:** identifica amenazas y vulnerabilidades técnicas sobre la plataforma tecnológica, propone controles técnicos y apoya la valoración del impacto sobre confidencialidad, integridad y disponibilidad.
- **Propietarios de los activos de información:** identifican riesgos sobre la información y procesos a su cargo, validan la valoración de los riesgos y aprueban las decisiones de tratamiento (mitigar, aceptar, etc.) sobre sus activos.

Registros resultantes:

- Metodología de análisis y tratamiento de riesgos.
- Matriz de riesgos de seguridad de la información.
- Plan de Tratamiento de Riesgos.
- Declaración de Aplicabilidad.
- Actas con resultados y decisiones sobre riesgos.

6.5 Definición, revisión y aprobación de políticas y procedimientos

Actividad: Elaborar, revisar y aprobar las políticas y procedimientos de seguridad de la información que soportan el Plan.

Cómo se realiza:

1. Con base en los resultados de riesgos y en los requisitos de ISO/IEC 27001:2022, la Oficina de Sistemas y la Oficina de Control Interno proponen o actualizan políticas y procedimientos (organización de la seguridad, seguridad del personal, gestión de activos, acceso, criptografía, seguridad física, operaciones, comunicaciones, privacidad y datos personales, etc.).
2. Las propuestas se presentan al CSI para análisis técnico y recomendación.
3. La Alta Dirección revisa y aprueba formalmente las políticas.
4. Talento Humano y Control Interno coordinan la socialización y capacitación al personal.
5. Se establece al menos una revisión anual o cuando se presenten cambios significativos (normativos, tecnológicos o de riesgos).

La elaboración, revisión, socialización y actualización de políticas y procedimientos estará condicionada a que la Alta Dirección disponga el tiempo de los responsables y los recursos mínimos necesarios para su desarrollo, divulgación y cumplimiento.

Responsables:

- **Alta Dirección:** revisa y aprueba formalmente las políticas y procedimientos de seguridad de la información, asigna recursos para su implementación y exige su cumplimiento.
- **Comité de Seguridad de la Información:** analiza técnicamente las propuestas de políticas/procedimientos, verifica su coherencia con los riesgos y con ISO/IEC 27001:2022, y emite recomendaciones de aprobación o ajuste.
- **Oficina de Sistemas de Información:** redacta y actualiza políticas y procedimientos de carácter técnico (acceso, redes, copias, malware, etc.), asegurando su viabilidad operativa.

- **Oficina de Control Interno:** vela por la alineación de las políticas con la normatividad aplicable, riesgos identificados y resultados de auditorías; propone ajustes cuando se detectan debilidades.
- **Oficinas de Contratación y Talento Humano:** incorporan las políticas de seguridad de la información en procesos de contratación, vinculación, capacitación y cláusulas contractuales; coordinan la socialización a los colaboradores y terceros.

Registros resultantes:

- Políticas y procedimientos aprobados con su control de cambios.
- Actas de CSI y de Gerencia donde se aprueban políticas.
- Evidencias de socialización y capacitación (listas de asistencia, material de apoyo).

6.6 Implementación de controles organizacionales y de personal

Actividad: Implementar las actividades asociadas a los controles organizacionales y de personas definidos en el Plan y en ISO/IEC 27001:2022 (controles de los dominios A.5 y A.6).

Cómo se realiza:

1. **Vinculación y desvinculación:**
   - Talento Humano y Contratación verifican antecedentes, gestionan la firma de acuerdos de confidencialidad y aceptación de políticas.
   - En desvinculación o cambio de funciones, se ejecuta el procedimiento de retiro: revocación de accesos, devolución de activos, actualización de inventarios y paz y salvo.
2. **Concientización y capacitación:**

- Control Interno diseña y ejecuta el programa anual de concientización en seguridad de la información.
- Talento Humano convoca, registra asistencia y aplica sanciones por inasistencia injustificada.

3. Responsabilidades disciplinarias:

- Se aplican los procedimientos disciplinarios cuando se identifiquen violaciones a las políticas de seguridad de la información.

Responsables:

- **Oficinas de Contratación y Talento Humano**: aplican verificaciones previas a la vinculación, gestionan la firma de acuerdos de confidencialidad y aceptación de políticas, y coordinan el proceso de desvinculación (retiro, cambio de cargo, licencias).
- **Oficina de Control Interno**: diseña, coordina y evalúa el programa de concientización y capacitación en seguridad de la información, y verifica el cumplimiento de las políticas por parte del personal.
- **Oficina de Control Interno Disciplinario**: adelanta los procesos disciplinarios cuando se evidencian violaciones a las políticas de seguridad de la información y recomienda sanciones de acuerdo con la gravedad de los hechos.
- **Subgerentes, Coordinadores, y jefes**: velan por que su personal conozca, aplique y cumpla las políticas; autorizan accesos a la información y reportan oportunamente cambios de funciones o desvinculaciones.

Registros resultantes:

- Hojas de vida con soportes.
- Acuerdos de confidencialidad y aceptaciones de políticas firmados.
- Registros de capacitación (programas, listas de asistencia).
- Registros de procesos disciplinarios relacionados con seguridad de la información.
- Formatos de retiro y paz y salvo por devolución de activos.

6.7 Implementación de controles físicos y de equipos

Actividad: Proteger físicamente las instalaciones, áreas seguras y equipos, de acuerdo con los controles del dominio físico.

Cómo se realiza:

1. Definir áreas seguras (centro de cómputo, centros de cableado, áreas de procesamiento de información sensible) e implementar controles de acceso físico (carnés, cerraduras, cámaras, registro de visitantes, etc.).
2. Coordinar con Recursos Físicos las condiciones ambientales adecuadas: climatización, detección y extinción de incendios, sistemas de descarga eléctrica y vigilancia.
3. Restringir accesos físicos no autorizados a equipos y áreas sensibles.
4. Controlar la entrada y salida de equipos de cómputo y otros recursos tecnológicos mediante autorizaciones formales y actualización del inventario.

La puesta en marcha y el mantenimiento de los controles físicos descritos estarán sujetos a la disponibilidad y aprobación de recursos por parte de la Gerencia y la Subgerencia Administrativa, especialmente en lo relacionado con adecuaciones de infraestructura, adquisición de dispositivos de seguridad y servicios de mantenimiento.

Responsables:

- **Oficina de Sistemas de Información:** identifica las áreas que requieren tratamiento como áreas seguras, define requisitos técnicos para la protección de equipos y coordina con Recursos Físicos la implementación de controles físicos.
- **Almacén**: implementa y mantiene los controles físicos y ambientales (acceso físico, cerraduras, cámaras, alarmas, climatización, detección/extinción de incendios, etc.) en las áreas definidas.

- **Área de Activos Fijos**: controla la entrada, salida y traslado de equipos de cómputo y otros recursos tecnológicos, manteniendo actualizado el inventario y las evidencias de movimiento.
- **Subgerentes, Coordinadores, y jefes**: supervisan el respeto a las restricciones de acceso físico en sus áreas y reportan anomalías o vulneraciones a los controles físicos implementados.

Registros resultantes:

- Listas de áreas seguras y controles asociados.
- Bitácoras de ingreso a centro de cómputo y centros de cableado.
- Registros de mantenimiento de sistemas físicos y ambientales.
- Formatos de movimiento de activos y de autorización de salida de equipos.

6.8 Implementación de controles tecnológicos y de acceso

Actividad: Gestionar el acceso lógico a redes, sistemas y aplicaciones, así como otros controles tecnológicos.

Cómo se realiza:

1. **Gestión de cuentas de usuario y privilegios:**
   - Jefes inmediatos y propietarios de sistemas solicitan creación, modificación, bloqueo y eliminación de cuentas.
   - Oficina de Sistemas crea cuentas conforme a perfiles definidos, aplica políticas de contraseñas y revisa periódicamente los accesos (incluyendo cuentas de altos privilegios).
2. **Uso de dispositivos móviles, periféricos y medios de almacenamiento:**
   - Sistemas define configuraciones seguras, cifrado, bloqueo automático, antivirus y borrado remoto de equipos móviles.

- Se regulan y autorizan los periféricos y medios de almacenamiento institucionales.

3. Tokens y firmas digitales:

- Se gestionan solicitudes, entrega y custodias de tokens y firmas, así como su revocación en caso de pérdida, robo o retiro del funcionario.

4. Seguridad de redes, correo e Internet:

- Se configuran dispositivos de seguridad de red y se segmentan las redes.
- Se administran cuentas de correo institucional, filtros antispam y antimalware.
- Se controlan los sitios de Internet permitidos y se registran los accesos.

La implementación y sostenimiento de estos controles tecnológicos dependerán de la asignación de recursos para adquisición y renovación de licencias, equipos y servicios necesarios, decisión que corresponde a la Gerencia y a la Subgerencia Administrativa con base en la priorización de riesgos y necesidades institucionales.

Responsables:

- **Oficina de Sistemas de Información**: administra la creación, modificación, bloqueo y eliminación de cuentas de usuario; configura políticas de contraseñas, segmenta redes, administra correo e Internet, y define parámetros de seguridad para dispositivos, medios y tokens.
- **Propietarios de sistemas de información:** definen perfiles de acceso y privilegios funcionales necesarios para sus sistemas, autorizan las solicitudes de acceso de sus usuarios y revisan periódicamente que los privilegios asignados sigan siendo pertinentes.
- **Subgerentes, Coordinadores, y jefes:** solicitan formalmente los accesos para su personal, verifican su necesidad funcional y controlan que los usuarios hagan un uso adecuado de los recursos tecnológicos y de acceso otorgados.

Registros resultantes:

- Formularios de solicitud de usuarios y perfiles.

- Listados actualizados de cuentas (incluyendo cuentas administrativas).
- Registros de entrega/recepción de equipos, tokens y medios de almacenamiento.
- Registros de configuración de dispositivos de red y seguridad.
- Logs de acceso a red, sistemas, correo e Internet.

6.9 Operación diaria, copias de respaldo y protección frente a software malicioso

Actividad: Operar y administrar la plataforma tecnológica de forma segura, asegurando copias de respaldo y protección contra software malicioso.

Cómo se realiza:

1. Sistemas documenta y ejecuta los procedimientos operativos (mantenimientos, monitoreo, capacity planning, etc.).
2. Se implementan herramientas antivirus, antimalware, antispam y antispyware, aplicando actualizaciones periódicas en toda la plataforma.
3. Se prohíbe a los usuarios modificar la configuración de estas herramientas.
4. Se implementa y ejecuta la estrategia de copias de respaldo: frecuencia, tipo (completa/incremental), rotación, sitio alterno de almacenamiento, pruebas periódicas de restauración.
5. Se documentan y atienden los incidentes de fallas de hardware, software o contagio de malware, gestionados a través de Tikects.

La operación segura de la plataforma tecnológica, la ejecución de copias de respaldo y el mantenimiento de las soluciones de protección frente a software malicioso estarán supeditadas a la asignación de recursos por parte de la Alta Dirección para licenciamiento, almacenamiento, servicios de backup.

Responsables:

- **Oficina de Sistemas de Información:** documenta y ejecuta procedimientos operativos, administra herramientas de seguridad (antivirus, antimalware, antispam, etc.), diseña y mantiene la estrategia de copias de respaldo, y coordina pruebas de restauración.
- **Mesa de Ayuda / Soporte:** recibe, registra y atiende solicitudes e incidentes relacionados con fallas de hardware, software o sospechas de malware; escala los casos según los procedimientos establecidos.
- **Propietarios de sistemas de información**: definen qué información de sus sistemas es crítica y debe respaldarse, validan la periodicidad de copias y participan en pruebas de restauración para asegurar la continuidad de sus procesos.

Registros resultantes:

- Procedimientos operativos documentados.
- Registro de tareas de mantenimiento preventivo y correctivo.
- Registros de copias de respaldo (planes, bitácoras de ejecución, pruebas de restauración).
- Informes de incidencias de software malicioso y acciones tomadas.

6.10 Intercambio de información y relaciones con terceros

Actividad: Gestionar de forma controlada el intercambio de información con terceros y el tratamiento de datos personales.

Cómo se realiza:

1. Contratación y Control Interno definen y actualizan modelos de Acuerdos de Confidencialidad y de Intercambio de Información para proveedores, aliados y otras entidades.

2. Toda transferencia de información (física o digital) con terceros se realiza utilizando medios autorizados, cifrado cuando aplique y con trazabilidad de emisor, receptor, fecha y contenido.
3. Las áreas que tratan datos personales obtienen la autorización de los titulares y aplican las políticas de tratamiento y protección de datos personales, en cumplimiento de la Ley 1581 de 2012 (Congreso de la República de Colombia, 2012).
4. Se supervisa el cumplimiento de los acuerdos por parte de los terceros, incluyendo la destrucción segura de la información una vez cumplida su finalidad.

Responsables:

- **Área de Contratación:** incluye cláusulas de confidencialidad e intercambio de información en los contratos, gestiona la firma de acuerdos con terceros y verifica contractualmente el cumplimiento de las obligaciones de protección de la información.
- **Oficina de Control Interno**: define procedimientos para intercambio de información, supervisa el cumplimiento de los acuerdos por parte de terceros y recomienda acciones cuando se detectan incumplimientos o riesgos.
- **Propietarios de activos de información**: autorizan las solicitudes de entrega/recepción de información a terceros, determinan qué información puede compartirse y en qué condiciones, y verifican la destrucción o devolución de la información cuando ya no se requiere.
- **Coordinación de Gestión Documental**: gestiona el envío y recepción de documentos físicos y medios de almacenamiento, asegura el uso de servicios de mensajería autorizados y mantiene registro de las transferencias.
- **Oficina de Sistemas de Información**: provee canales seguros para intercambio digital de información (cifrado, repositorios seguros, conexiones controladas) y apoya la trazabilidad de estas transferencias.

Registros resultantes:

- Modelos y ejemplares firmados de Acuerdos de Confidencialidad y de Intercambio de Información.
- Registros de envío/recepción de información (guías de mensajería, actas de entrega, trazas de transferencia).
- Registros de autorización de tratamiento de datos personales.
- Evidencias de destrucción de información a cargo de terceros.

6.11 Gestión de incidentes de seguridad de la información y sanciones

Actividad: Detectar, reportar, analizar y tratar incidentes de seguridad de la información, así como aplicar las sanciones correspondientes cuando se violen las políticas.

Cómo se realiza:

1. Los usuarios reportan de manera inmediata cualquier incidente o sospecha de incidente a la Gerencia, Oficina de Sistemas o Mesa de Ayuda, siguiendo el procedimiento establecido.
2. La Oficina de Sistemas de Información analiza el incidente (impacto, causa raíz, sistemas afectados) y define acciones de contención, mitigación y recuperación.
3. Cuando corresponda, el CSI y Control Interno evalúan el incidente y definen medidas adicionales, incluyendo la notificación a autoridades competentes.
4. La Oficina de Control Interno Disciplinario analiza si hay méritos para abrir proceso disciplinario según la gravedad del incidente y el incumplimiento de las políticas.

Responsables:

- **Todos los usuarios:** detectan y reportan de inmediato cualquier incidente o sospecha de incidente de seguridad de la información, utilizando los canales definidos (Mesa de Ayuda, Sistemas, Gerencia).

- **Oficina de Sistemas de Información:** realiza el análisis técnico del incidente, aplica medidas de contención, mitigación y recuperación, y documenta las acciones ejecutadas y lecciones aprendidas.
- **Comité de Seguridad de la Información:** analiza incidentes relevantes o repetitivos, evalúa su impacto en el SGSI y define acciones de mejora o cambios en políticas y controles.
- **Oficina de Control Interno:** evalúa el incidente desde la perspectiva de cumplimiento y controles internos, recomienda acciones correctivas y hace seguimiento a su implementación.
- **Oficina de Control Interno Disciplinario:** determina, cuando corresponda, la apertura de procesos disciplinarios y aplica las sanciones definidas en la normatividad interna.
- **Gerencia**: toma decisiones de alto nivel en incidentes de alto impacto.

Registros resultantes:

- Formatos de reporte de incidentes.
- Bitácoras de atención de incidentes y acciones correctivas.
- Informes de incidentes relevantes al CSI y a la Gerencia.
- Registros de procesos disciplinarios asociados a incidentes de seguridad.

6.12 Registro de eventos, auditoría interna y mejora continua

Actividad: Monitorear el desempeño del Plan mediante registros de eventos, auditorías y revisiones, y aplicar acciones de mejora continua.

Cómo se realiza:

1. Sistemas y Control Interno definen qué eventos se deben registrar en los logs de auditoría (accesos, cambios de configuración, fallas de autenticación, acciones administrativas, etc.) y los periodos de retención.

2. Se habilitan y administran los mecanismos de registro en los sistemas y dispositivos relevantes.
3. Control Interno revisa periódicamente los registros para identificar brechas de seguridad, incumplimientos o comportamientos anómalos.
4. Se ejecuta un programa anual de auditorías internas al SGSI/Plan de Seguridad y Privacidad de la Información, revisando cumplimiento de políticas, procedimientos y controles.
5. La Gerencia y el CSI realizan la revisión por la dirección, analizando resultados de auditorías, incidentes, riesgos, avances de planes de tratamiento y oportunidades de mejora.
6. Se definen y ejecutan acciones correctivas y de mejora y se actualizan los documentos del Plan cuando sea necesario.

Responsables:

- **Oficina de Sistemas de Información:** configura y administra los registros de eventos (logs) en sistemas, redes y aplicaciones; garantiza su integridad y disponibilidad, y apoya el análisis técnico de dichos registros.
- **Oficina de Control Interno**: define los eventos críticos a monitorear, los periodos de retención de logs, revisa periódicamente la información registrada y coordina las auditorías internas relacionadas con seguridad de la información.
- **Comité de Seguridad de la Información**: recibe los resultados de auditorías, revisiones de logs e indicadores de desempeño del Plan; propone y prioriza acciones de mejora.
- **Gerencia**: revisa periódicamente el desempeño del Plan (revisión por la dirección), aprueba acciones correctivas y de mejora y define prioridades estratégicas en materia de seguridad de la información.

Registros resultantes:

- Configuración de logs y bitácoras de auditoría.

- Informes de monitoreo y análisis de logs.
- Plan anual de auditorías internas y sus informes.
- Actas de revisión por la dirección / CSI.
- Planes de acción y registros de acciones correctivas y de mejora.

6.13 Programa de auditoría interna del Plan de Seguridad y Privacidad de la Información

La E.S.E. RAFAEL TOVAR POVEDA realizará auditorías internas periódicas al Plan de Seguridad y Privacidad de la Información y al Sistema de Gestión de Seguridad de la Información, con el fin de:

- Verificar el cumplimiento de las políticas, normas y procedimientos establecidos.
- Evaluar la eficacia de los controles implementados.
- Identificar oportunidades de mejora y necesidades de ajuste del Plan.

Como regla general, las auditorías internas se realizarán al menos una vez al año, o cuando se presenten cambios significativos en la estructura organizacional, en los activos de información estratégicos o en la normatividad aplicable.

Responsables:

- La Oficina de Control Interno es responsable de planear, coordinar y ejecutar el programa de auditoría interna en materia de seguridad de la información, de acuerdo con la normatividad vigente para las Entidades Sociales del Estado.
- Dada la complejidad técnica de la seguridad de la información y de las normas internacionales aplicables, cuando la E.S.E. no cuente con personal interno con la competencia necesaria en seguridad de la información y en normas como ISO/IEC 27001, la E.S.E. deberá considerar prioritario apoyarse en auditores o consultores

externos especializados, que acrediten experiencia y formación en dicha norma. Este apoyo externo permitirá:

- Asegurar la independencia frente a las áreas auditadas.
- Contar con criterios actualizados y buenas prácticas reconocidas internacionalmente.
- Elevar el nivel técnico de las auditorías internas y la calidad de las recomendaciones emitidas.

Registros resultantes:

- Plan anual de auditoría interna.
- Listas de verificación y documentos de trabajo de auditoría.
- Informes de auditoría interna de seguridad de la información.
- Planes de acción derivados de los hallazgos y su seguimiento.

La ejecución de las actividades descritas en este numeral, así como la implementación y mantenimiento de los controles definidos en el Plan de Seguridad y Privacidad de la Información, está condicionada a la disponibilidad y asignación de recursos humanos, tecnológicos, físicos y financieros por parte de la Alta Dirección de la E.S.E. RAFAEL TOVAR POVEDA. Cuando los recursos mínimos necesarios para implementar un control o actividad no puedan ser asignados en el tiempo requerido, esta situación deberá registrarse expresamente en la matriz de riesgos de seguridad de la información y/o en las actas del Comité de Seguridad de la Información o del órgano que haga sus veces, indicando el riesgo residual asociado y las decisiones adoptadas por la Gerencia. De esta manera, la E.S.E. asegura la trazabilidad de las decisiones, el cumplimiento del enfoque basado en riesgos establecido por la norma ISO/IEC 27001:2022 y el compromiso de la Alta Dirección con la mejora continua del Sistema de Gestión de Seguridad de la Información.

7. CRONOGRAMA DE ACTIVIDADES

El cronograma de actividades del Plan de Seguridad y Privacidad de la Información es la herramienta de planificación que organiza, en el tiempo, las acciones definidas en el presente documento (especialmente las descritas en el numeral 6), indicando responsables, periodos de ejecución, recursos requeridos y evidencias, con el fin de facilitar su gestión, seguimiento y mejora continua.

Este cronograma se elabora, como mínimo, con periodicidad anual y se encuentra alineado con:

- El ciclo PHVA (Planear – Hacer – Verificar – Actuar) del Sistema de Gestión de Seguridad de la Información.
- Los resultados del análisis y tratamiento de riesgos de seguridad de la información.
- La disponibilidad de recursos humanos, tecnológicos, físicos y financieros definidos por la Alta Dirección.

7.1 Lineamientos para la elaboración del cronograma

Para la elaboración del cronograma de actividades se tendrán en cuenta, como mínimo, las siguientes directrices:

1. Fuente de actividades:

- Las actividades por programar se derivan de las responsabilidades y acciones descritas en el numeral 6 del presente Plan, de los planes de tratamiento de riesgos, de los resultados de auditorías internas y externas, y de las necesidades identificadas por el Comité de Seguridad de la Información (CSI) y la Gerencia.

2. Planeación anual:

- El cronograma se construye para un periodo anual, pudiendo ajustarse cuando se presenten cambios significativos en los riesgos, en la infraestructura tecnológica, en la normatividad aplicable o en la estructura organizacional.

3. Contenido mínimo:

Cada actividad del cronograma debe contener, como mínimo:

- Descripción de la actividad.
- Dependencia responsable y responsable directo.
- Relación con el numeral correspondiente del Plan y/o con el riesgo asociado.
- Periodo de ejecución (fecha de inicio y fin) y frecuencia.
- Recursos requeridos (humanos, tecnológicos, físicos y/o financieros).
- Producto o evidencia esperada (registro, informe, acta, formato, etc.).
- Indicador o criterio de cumplimiento.

4. Aprobación y seguimiento:

- El cronograma será consolidado por la Oficina de Sistemas de Información y la Oficina de Control Interno, revisado por el Comité de Seguridad de la Información y aprobado por la Gerencia.
- El avance de las actividades programadas será revisado periódicamente en las sesiones del CSI y/o en los espacios de seguimiento institucional que se definan, registrando los avances, dificultades y acciones de mejora.

7.2 Anexo: Formato Planeación Anual de Actividades

Las actividades del Plan de Seguridad y Privacidad de la Información deberán quedar soportadas en un cronograma de actividades diligenciado en el formato institucional:

“Planeación Anual de Actividades – Plan de Seguridad y Privacidad de la Información”

El formato mencionado hace parte integral del presente Plan como anexo, y será el documento de referencia para:

- La programación anual de las actividades del Plan.
- El registro de responsables, periodos de ejecución, recursos y evidencias.
- El seguimiento y cierre de las actividades planificadas.

La Gerencia y la Subgerencia Administrativa deberán asegurar que el cronograma cuente con la asignación de recursos mínimos necesarios para su ejecución y, cuando no sea posible asignarlos en el tiempo requerido, esta situación se registrará como riesgo residual en la matriz de riesgos de seguridad de la información y/o en las actas del Comité de Seguridad de la Información.

8. BIBLIOGRAFIA

- Congreso de la República de Colombia. (2000). Ley 594 de 2000. Por la cual se dicta la Ley General de Archivos. Diario Oficial de la República de Colombia.
- Congreso de la República de Colombia. (2008). Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países.
- Congreso de la República de Colombia. (2009). Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado: de la protección de la información y de los datos, y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones. Diario Oficial de la República de Colombia.
- Congreso de la República de Colombia. (2012). Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial de la República de Colombia.
- Constitución Política de Colombia. (1991). Constitución Política de Colombia. Bogotá, Colombia.
- ICONTEC. (2009). NTCGP 1000:2009. Norma Técnica de Calidad en la Gestión Pública. Instituto Colombiano de Normas Técnicas y Certificación.
- International Organization for Standardization & International Electrotechnical Commission. (2004). ISO/IEC 13335-1:2004. Information technology—

Guidelines for the management of IT Security—Part 1: Concepts and models for IT security. ISO/IEC.

- International Organization for Standardization & International Electrotechnical Commission. (2022). ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection—Information security management systems—Requirements. ISO/IEC.
- Ministerio de Salud. (1999). Resolución 1995 de 1999. Por la cual se establecen normas para el manejo de la historia clínica. República de Colombia.

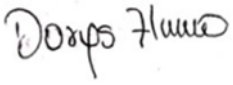
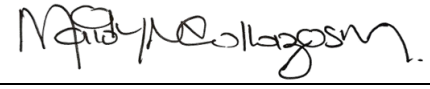
9. ANEXOS

Los siguientes documentos se consideran anexos y hacen parte integral del “Plan de Seguridad y Privacidad de la Información” de la E.S.E. RAFAEL TOVAR POVEDA. Estos anexos se administran en medio digital, de acuerdo con los lineamientos de gestión documental de la entidad.

Anexo 1. Formato “Planeación Anual de Actividades – Plan de Seguridad y Privacidad de la Información

Anexo 2. Procedimiento de confidencialidad de la información Laboratorio Clínico. Código: AP-GSI-AIF-PD001

CONTROL DE CAMBIOS		
Versión	**Descripción del Cambio**	**Fecha de aprobación**
01	Elaboración del documento	27/01/2020
02	Se ajusta documento por programa de auditoria para el mejoramiento continuo Pamec. Se ajusta objetivos, alcance, responsables, normatividad, se agrega en procedimiento describiendo la secuencia de las actividades necesarias para identificar, analizar, valorar y tratar los riesgos de seguridad y privacidad de la información. Por último, se ajusta plantilla según nueva versión del manual de gestión documental de calidad.	27/1/2026

Elaborado por:	Revisado por:	Aprobado por:
Firma: 	Firma: 	Firma: 
Nombre: Juan Camilo Guevara Plazas Cargo: Ingeniero de Sistemas	Nombre: Dorys Enith Almario Estrada Cargo: Asesora de Calidad	Nombre: Maidy Nayiver Collazos Medina Cargo: Subgerencia Administrativa y Financiera.